Detecting Malicious Dropping Attack in the Internet

Lata L. Ragha[1], B. B. Bhaumik[2], and S. K. Mukhopadhyay[3]
[1] Ramrao Adik Institute of Technology, Department of Computer Engineering, Nerul, Navi Mumbai, India
Email: lata.ragha@gmail.com
[2] Jadavpur University, Department of Computer Science and Engineering, Kolkata, India
Email: bbbhaumik@yahoo.com
[3] CA-30, Salt Lake, Sector-1, Kolkata-700064, India
Email: mukho_s@hotmail.com

***Abstract*— The current interdomain routing protocol, Border Gateway Protocol, is limited in implementations of universal security. Because of this, it is vulnerable to many attacks at the AS to AS routing infrastructure. Initially, the major concern about BGP security is that malicious BGP routers can arbitrarily falsify BGP routing messages and spread incorrect routing information. Recently, some authors have pointed out the impact of a type of attack, namely selective dropping or malicious dropping attack that has not studied before. The malicious draping attack can result in data traffic being blackholed or trapped in a loop. However, the authors did not elaborate on how one can detect such attacks. In this paper, we discuss and analyse a method that can be used to detect malicious dropping attacks in the Internet.**

***Index Terms*— Internet Routing Security, Selective or malicious Dropping Attacks, BGP, Instability Analysis, Malicious Routers.**

I. INTRODUCTION

Border Gateway Protocol (BGP) is the de facto interdomain routing protocol [1]. Current Internet consists of many Autonomous Systems (ASes) connected by interdomain (inter-AS) links. Each AS is a set of routers that have the same routing policy within a single administrative domain. BGP is responsible for discovery and maintenance of paths between ASes in the Internet. BGP routers exchange routing information via two types of UPDATE messages: namely route withdrawal and route announcement. When a BGP router receives an UPDATE from its neighboring BGP router, this message will be processed, stored, and redistributed in accordance with both BGP specification and the routing policies of the local AS.

Previously, the major concern about BGP security is the authenticity and integrity of BGP UPDATES, especially route origin information and AS path information stored in the AS_PATH attribute. Incorrect UPDATES, due to either BGP router misconfiguration or malicious attack, may cause serious problems to the global Internet. Some countermeasures have been proposed to mitigate BGP vulnerabilities. To protect BGP session from spoofed BGP UPDATES sent by outsiders, TCP MD5 signature [2] using shared secret key between two BGP routers was proposed. S-BGP[3] and SoBGP[4] apply cryptography to prevent an attacker (either insider or outsider) from advertising faulty BGP messages or tampering normal messages. However, as noted in [5], [6], [7], cryptography-based security mechanisms, cannot protect routing protocols against some kind of attacks. In [7], the authors describe one such attack, namely the malicious or selective dropping attack, which can cause data traffic blackhole and persistent traffic loop. However, the authors do not present any technique to detect such attacks.

In this paper, we describe a scheme, presented in [8], used for detecting Instability in BGP and by using the same technique we proposed a method for detecting malicious dropping attacks in the Internet. This scheme is based on adaptive segmentation of feature traces extracted from BGP update messages and exploiting the temporal and spatial correlations in the traces for robust detection of the instability events. The route change information is used to pinpoint the culprit ASes where the instabilities have originated. When this scheme cannot identify the instability source, it will probe its neighboring routers to see if they can identify the source of instability. Once the source of instability is identified, the stable route database will check to see if a malicious dropping attack is embedded within this burst of BGP UPDATES. If an attack is suspected, then a warning message will be flooded (with limited scope) across the BGP routers in the Internet.

II. MALICIOUS DROPPING ATTACK

BGP is a policy routing, path vector protocol. According to the inbound and outbound policies, BGP router may legitimately suppress some UPDATES. The authors in [7] define two consistency properties for correct BGP operation. In this model the notations: **peer(*u*)** denotes the set of peers for node (AS) *u*, **rib-in (*u*<=*w*)** denote node *u*'s most recently received message from peer *w*, **rib(*u*)** denotes the best path that *u* adopts and stores in the local-RIB, **rib**-out(*u*=>*w*) denotes the route that *u* advertises to *w*.

The properties defined by the authors in [7] are duplicated below:

1. a) If rib(*u*) □□□□□there must □v□□peers(*u*) [rib-in(*u*<=*v*)=rib(*u*)].
   b) If rib(*u*) =□□, rib-in(*u*<=*v*) can be arbitrary.
   □□□a) For any *w* □□peers(*u*), if rib-out(u=>w)□□□□□ then rib-out(*u*=>*w*) = u o rib(*u*).
   b) It is possible that when rib(*u*) □□□□, there exists

DOI: 01.IJNS.02.01.141

rib-out(u=>w) = □□where w □□peers(u).

The two properties listed above are legitimate properties that allow a BGP router at node u to drop BGP UPDATES. Property 1(a) implies node u can select a route from one peer but drop the routes it received from the others. Property 1(b) indicates that node u does not have to use the route announced by node v to reach a particular destination even though node u has no route. Property 2(a) guarantees that no policy allows node u to use one route but announce the other route to its peers. Property 2(b) indicates a policy to authorize node u not to transit the traffic for node v even though node u can reach a particular destination.

Any BGP dropping that is not consistent to these two properties will be classified as malicious dropping. The and this can result in traffic blackhole and persistent traffic loop.

A. Blackhole

In the example network shown in Figure 1, we assume that each node represents an AS, there is a BGP router associated with each AS.

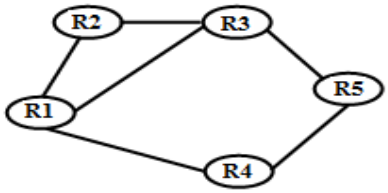

Figure 1. Example network to show blackhole and rooting loop

The target network is owned by AS5. We study the routes to this network in five BGP routers. In the initial stable state, R1 uses (AS3, AS5) as the best AS path to reach the target network. R1 uses R3 as the next hop. When we cut the link between R3 and R5, under normal circumstances, R1 will remove (AS3, AS5) from the BGP routing table and select (AS4, AS5) the best path. This path will be announced to AS2, which will use the path (AS1, AS4, AS5). In the forwarding table, for the entry of the particular network of AS5, R1 sets R4 as the next hop, R2 and R3 set R1 as the next hop. However, if R3 is malicious, it can hijack the normal traffic to the target network by malicious dropping attack. In this example, we let R3 hold the withdrawal messages to R1 and only send a withdrawal message to R2. Consequently, although R1 receives the route withdrawal from R2, it will still use R3 as next hop to deliver traffic to the network of AS5. Therefore, all the traffic from AS1 will be blackholed by R3.

B. Routing Loop

The same example network is used to explain about the persistent routing loop. The target network is still considered in AS5. The major difference from the first example network is that R3 is a normal node whereas R1 is malicious. R1 selectively drops outgoing route announcements to R2 in the beginning. In the example, R1 sets (AS3, AS5) as the best path, yet drops the route update to R2. It announces (AS1, AS4, AS5) to R2 instead of announcing the current route stored in the Loc-RIB. R3 announces (AS3, AS5) to R2. R2 sets a larger local preference value to the route learned from R1 than the route learned from R3 so that R2 uses (AS1, AS4, AS5) as the best AS path. Initially, in the stable state, every router chooses the correct next hop for the destination network.

Same as the first example, we cut the link between R3 and R5. Consequently, R3 sends route withdrawal to R1 and R2. R1 maliciously drops this incoming message and still uses the route (AS3, AS5). When R2 receives the withdrawal message, R2 uses the route (AS1, AS4, AS5) and sends this route back to R3. Finally, R3 uses the route (AS2, AS1, AS4, AS5). From the routing policies, we can see that the loop has been formed. For the route to AS5, R3 sets R2 as next hop, R2 sets R1 as next hop, R1 sets R3 as next hop.

III. SECURITY SOLUTIONS

The solution space for securing the global routing system can be broadly divided into three areas: prevention, mitigation, and detect-and-react.

A. Prevention

The proposed secure BGP solutions in this category are based on cryptographic authentications [3], [9], [10], [11]. Unfortunately these solutions share some obstacles and effectively blocked the road towards actual deployment.

- The absence of a global PKI infrastructure in today's Internet,
- The high computational overhead of verifying BGP update signatures,
- The requirement of changing implementations of all routers to achieve effective protection.

B. Mitigation

Even though many authors proposed different approaches to mitigate the attacks [12], [13], [14] through observing each router for the origin ASes and AS paths of the routes over time, and defer the adaption to any sudden route changes till the changes can be verified through other means, these approaches does not scale as a general solutions for all prefixes.

C. Detect-and-React

Over the years a number of detection-based security solutions have been developed [13], [15], [16] and even deployed. All the techniques usually have two basic components: a monitoring infrastructure that collects BGP routing update information, and a user profile that provides the ground truth of the network being observed. One fundamental advantage of detection-based mechanisms is the ease of deployment and they do not require any change in the operational system. Any of the proposed solutions of instability detection in the Internet can be used to detect malicious dropping attacks.

IV. INSTABILITY DETECTION

A methodology for identifying the source of instability is described in literature [8]. The scheme is based on adaptive segmentation of feature traces extracted from BGP update messages and exploiting the temporal and spatial correlations in the traces for robust detection of the

DOI: 01.IJNS.02.01.141

instability events. Then the route change information is used to pinpoint the culprit ASes where the instabilities have originated.

A System Architecture

This section presents a description of the architecture of the system and its components and their functions [8]. This system can be broadly described as a two part scheme: the first part detects the BGP instability events while the second pinpoints the source of the instability.

Feature Extractor: It performs the basic function of parsing the needed features from the BGP update messages received by a router from its peers. It separates the update messages received from different peers into different datasets and then performs the necessary parsing on these datasets to obtain the feature traces. The features are extracted on data collected every 5 minutes in order to limit the rate at which data needs to be processed.

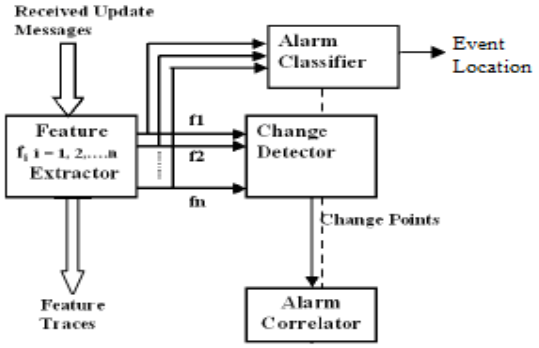

Figure 2. Architecture of the detection and root cause location scheme

Change Detector: The important function of tracking the behavior of the feature time series and detecting when a substantial change occurs in them is performed here. The change detection is performed for every feature trace extracted from each peer separately, in parallel.

Alarm Correlator: It is used to make the detection robust against feature volatility. It implements the algorithm to establish whether the alarms obtained from the different feature traces for the same peer are correlated. The correlation is checked across different combinations of features using a decision tree based mechanism.

Alarm Classifier: It helps in identifying the location of occurrence of the root cause event that caused the instabilities. It uses the AS-path data for this purpose.

B Feature Selection

When a route or node failure occurs, each BGP router initiates a path exploration process for the failed routes. The path exploration process involves the exchange of route withdrawal and announcement messages between BGP routers. These update messages show certain characteristics that are specific to periods of instability and form the features used by our instability detection mechanism. From the BGP update messages received by a router, authors identify and extract *features* that are used to differentiate between BGP's behavior during normal and anomalous periods

AS Path Length

Routing instabilities cause established paths to become unavailable or may result in certain destinations being unreachable. As a result, instabilities are characterized by route withdrawals and the BGP path exploration process to find an alternative route to the same destination.

Under such circumstances, it has been observed that the occurrence of many routes with abnormally long AS path lengths. This is because in the absence of stable paths of shorter lengths, BGP routers try to use longer alternative paths. Authors used the length of the AS paths received from a peer as one of features and define it as:

$$ASPL = \{ X_{ij} = (x_0, x_1, \ldots);\ i = 1,\ldots, M_l\ ;\ j = 1,\ldots, NP \}$$

Where, X_{ij} is a time series of the number of messages with AS path length = i, received over every 5 minute interval from peer number j, M_l is the maximum observed AS path length value and NP is the number of peers of the local BGP router.

AS Path Edit Distance

During instability, not only are a large number of long AS paths exchanged but also a large number of "rare" AS paths are advertised. We quantify the latter effect by treating AS paths received in consecutive messages as strings and obtaining edit distances between them as a measure of their dissimilarity. The AS path edit distance feature set is defined as:

$$ASPED = \{ X_{ij} = (x_0, x_1, \ldots);\ i = 1,\ldots, M_{ed}\ ;\ j = 1,\ldots, NP \}$$

Where, X_{ij} is a time series of the number of messages with AS path edit distance i, received over every 5minute interval from peer number j and M_{ed} is the maximum observed AS path edit distance value.

Message Volume

Interdomain routing instabilities also exhibit a sharp and sustained increase in the number of announcement and withdrawal messages exchanged by the BGP routers [8]. The volume of announcement and withdrawal messages as possible features that can be used to detect instabilities is considered. These features are defined as

$$AV_i = \{ X_i = [\ x(0), x(1),\ldots] \}, \forall i = 1,2,..,NP$$
$$WV_i = \{ Y_i = [\ y(0), y(1),\ldots] \}, \forall i = 1,2,..,NP$$

Where *Xi and Yi* are the time series of the number of announcements and withdrawals received in each interval from peer number i, respectively.

C Detection of Instabilities

This section describes the detection mechanism used in [8]. The detection scheme is based on adaptive sequential segmentation. The core of the segmentation is change detection using a Generalized Likelihood Ratio (GLR) based hypothesis test. The segment boundary detection mechanism uses the GLR test to detect change points. This step is followed by a process to optimize the segment boundary position (figure 3.

DOI: 01.IJNS.02.01.141

```
L   minimum initial window size;
δ   GLR threshold;
d(x,y)   GLR dist betn. windows [1,x] and [x+1,y];
s = L   initialize s as end of first learning
        and beginning of first test window;
while (sizeof(data) > 0) do
  while (d(s, s+L−1) < δ) do
      s = s+1   grow the learning and slide
                the test window by one sample;
  end while
  t_D = s+L−1   the change detection point;
  r = t_D − L+1   pointer to the beginning of
                current test window;
  for ( t_D − L+2 ≤ s ≤ t_D ) do
    g_1 = d(s, s+L−1)   GLR dist betn. growing
                learning and fixed test windows;
    g_2 = d(r, s+L−1)   GLR dist betn. fixed
                learning and growing test windows;
    if (g_1 > g_2) then
        r = s   found better boundary position;
    end if
    s = s+1
  end for
  ropt = r   optimal boundary position found;
  data = [data(r) : data(sizeof(data))]   further seg-
                mentation on remaining data;
end while
```

Figure 3. Algorithm for change detection and boundary position optimization [8]

The change detection and boundary position optimization processes of Algorithm shown in figure 3 are applied to each feature trace and the change points detected are termed *per-feature-trace* alarms. The temporal correlations between the per-feature-trace alarms are used to reduce false alarms and make the detection process more robust against volatility of feature traces. The clustering of the per-feature-trace alarms is done by using the time difference between them as a distance measure. Then a majority voting rule that requires the largest cluster to have alarms from more than half the number of feature traces is used to generate the final alarm.

D Detection of Root cause location

In order to locate the root-cause-AS, we need to find the *first-changed-AS*. The method that used here to find the first-changed-AS is an extension of the AS path edit distance feature extraction process.

E Detection of Malicious dropping attacks

The detection mechanism can be used to test and detect various types of instability events like: worm attack, equipment failure and BGP misconfiguration and hijack events. In case of hijacking if the downstream ASes did not have correct filters in plane, can cause a major instability and it is difficult to locate unique source of instability.

We use the same methodology described in [8] to extract BGP updates and locate the source of instability. The difference is when the locating instability procedure fails to locate a unique source of instability; we allow that observation point to probe its neighbors to see if they can identify the source of instability. Based on these additional information provided by its neighbors, an observation point may then be able to identify the source of instability. Next, this observation point will check its current routing table to see if the troubled inter-AS link is used in any current routing table. If this troubled link is used in any best-path route, then the detection module returns a true (indicating that there is a possible malicious dropping attack). Otherwise, the detection module returns a false (no indication of malicious dropping attack). The pseudo code of the malicious dropping attack detection module is explained below in Figure 4.

```
Detect_Dropping(u,t)//u is a cluster of updates at time period t {
// this is used to monitor AS to report instability and dropper
   instability=Locate(u); // running locating algorithm try to
                          // find instability
   if (instability == NULL) // if not found
   {instability=Ask_Neighbor(n, t); //ask peer  upto n hops
      if (instability == NULL)
      {   error("can't find instability!"); return; }
   }
     report instability, t; // if instability found
     dropper=Check_RT(instability, current_node);
     if (dropper != NULL)
       { report dropper, t;  return;  }
   return;
}
```

Figure 4: Malicious dropping attack detection procedure

We illustrate our proposed attack detection method using an example based on the network topology shown in Figure 5. We assume that each node represents an AS, there is a BGP router associated with each AS and there is a BGP peer session between the BGP routers if there is a link exists between two nodes.

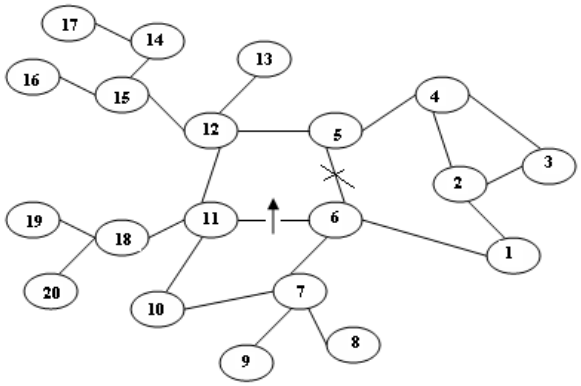

Figure 5. Example of network topology

Assume that link 5-6 is broken and this results in a burst of BGP update messages. If there is no malicious/selective dropping attack**,** and the proposed method is implemented in any one of the routers, the source of instability can be easily located and the alarm message will be issued to all the routers. However, if the link 5-6 is broken and at the same time, the router in AS6 launches a malicious dropping attack towards AS11, then ASes 11, 18, 19, 20 cannot locate the source of the instability. AS11 can verify the source of instability after it has asked its neighboring routers i.e. AS10 and AS12 for information on the source of instability that they have identified for the same burst. Upon receiving the information from AS10 and AS12,

DOI: 01.IJNS.02.01.141

AS11 was able to check its routing table and discover a discrepancy about the status of the inter-AS link 5-6. Thus, AS11 was able to detect a potential malicious/selective dropping attack. AS11 can then issue a warning message which is propagated with limited scope across the network. The warning message contains information about the identifier of the malicious router and any suspected broken links that are not reported. Such warning messages are authenticated so that attackers will not issue forged warning messages to confuse neighbors. BGP router identity authentication approach proposed in S-BGP[4] can be used for authenticating warning messages.

In the above example, without the neighbour probing technique**, five** of the AS routes will use an AS path that goes through the broken link as a result of the malicious dropping attack. With the neighbour probing technique, only **three** of the AS routes will use an AS path that goes through the broken link if no warning message is issued. If the warning message is flooded across the whole network, then no AS will utilize a path that goes through the broken inter-AS link and hence the damaged cost is reduced to 0. One potential limitation of this technique is that unless a router has peers with at least 2 or 3 other routers, this router will not be able to get additional information to help it locate the source of instability as well as detect any potential malicious router that selectively drops BGP updates.

F Implementation

Initially we are planning to implement the proposed method in NS-BGP simulator and later by using SSFNet. We are thinking for the topology with different weights for different AS links based on the traffic load each carries or the number of different AS routes that use a particular AS link. We are also thinking of possible solutions to address several issues:

First, we need to propose a method for adding two new BGP message types for neighbor probing and warning purposes. Next, one needs to carefully think about the scope of the warning message distribution.

V. CONCLUSION

In this paper, we have described a method used for detecting instabilities in the internet along with detection of root cause location. We also explained a neighbor probing scheme for detecting malicious dropping attacks in the Internet. The different network topologies have been theoretically analyzed to evaluate the effectiveness of our proposed scheme. It is further analyzed that when the method detects the presence of potential malicious router, the damage cost can be reduced to certain percentage without deploying the warning message. With the warning message, the damaged cost can be reduced to zero. We intend to implement and analyze this proposed method by using NS-BGP simulator.

REFERENCES

[1] Y. Rekhter and T. Li, "Border Gateway Protocol 4", RFC 1771, SRI Network Information Center, July, 1995.

[2] A. Heffernan, "Protection of BGP sessions via the TCP MD5 signature option", RFC 2385, SRI Network Information Center, August, 1998

[3] S. Kent et al, "Secure Border Gateway Protocol (S-BGP)", IEEE Journal on Selected Areas in Communications, Volume18 Issue 4, April, 2000

[4] C. Kruegel et al, "Topology-based detection of anomalous BGP messages", Proceedings of 6th Symposium on Recent Advanced in Intrusion Detection (RAID), 2003.

[5] S. M. Belovin and E. R. Gansner, "Using Link Cuts to attack Internet Routing", draft, May 2003.

[6] S. M. Belovin, "Routing Security", Talk at British Columbia Institute of Technology, June 2003.

[7] K. Zhang, X. Zhao, F. Wu, "An analysis of Selective Dropping Attack in BGP", Proceedings of IEEE IPCCC, April, 2004.

[8] Shivani Deshpande, Marina Thottan, Tin K. H. And Biplab Sikdar, "An Online Mechanism for BGP Instability Detection and Analysis", IEEECSI, 2009.

[9] J. Ng. "Extensions to BGP to Support Secure Origin BGP", fttp://ftpeng.cisco.com/sobgp/drafts/draft-ng-sobgp-bgp-extensions-02.txt, April 2004.

[10] G. Huston and G. Michaelson, "Validation of Route Origination in BGP using the Resource Certificate PKI", Internet Draft, IETF, 2008.

[11] S. S. M. Zhao and D. Nicol, "Aggregated path authentication for efficient BGP Security", in 12th ACM Conference on Computer and Communications Security, November 2005.

[12] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, A. Mankin, S. Wu, and L. Zhang, " Protecting BGP Routes to Top Level DNS Servers", in Proceedings of the ICDCS 2003.

[13] J. Karlin, S. Forrest, and J. Rexford, "Pretty good BGP: Improving BGP by cautiously adopting routes", in Proceedings of the 14th IEEE International Conference on Network Protocols, 2006.

[14] Z. Zhang, Y. Zhang, Y. C. Hu, and Z. M. Mao, "Practical defenses against BGP prefix hijacking", in Proceedings of the ACM CoNEXT conference, 2007.

[15] Y. J. Chi, R. Oliveira, and L. Zhang, "Cyclops: the AS-level connectivity observatory", SIGCOMM Computer Communications, 2008. http://cyclops.cs.ucla.edu.

[16] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, "PHAS: A prefix hijack alert system" in 15th USENIX Security Symposium, 2006.

DOI: 01.IJNS.02.01.141